



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets ⁶ :

H04L 9/32, G07F 7/10

A1

(11) Numéro de publication internationale:

WO 98/13972

(43) Date de publication internationale:

2 avril 1998 (02.04.98)

(21) Numéro de la demande internationale: PCT/FR97/01687

(22) Date de dépôt international: 25 septembre 1997 (25.09.97)

(30) Données relatives à la priorité:

96/11916

25 septembre 1996 (25.09.96)

FR

(71) Déposant (pour tous les Etats désignés sauf US): FINTEL S.A.
[FR/FR]; 87, boulevard Haussmann, F-75008 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (US seulement): ROSSET, Franck
[FR/FR]; 96, boulevard Beaumarchais, F-75011 Paris (FR).
GAYET, Alain [FR/FR]; 13, place des Dominos, F-92400
Courbevoie (FR). MOULIN, Jean [FR/FR]; 5, avenue de
Beauséjour, F-92210 Draveil (FR).(74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Im-
meuble Germanium, 80, avenue des Buttes de Coësmes,
F-35700 Rennes (FR).(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY,
CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH,
HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR,
LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ,
PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR,
TT, UA, UG, US, UZ, VN, YU, ZW, brevet ARIPO (GH,
KE, LS, MW, SD, SZ, UG, ZW), brevet eurasién (AM, AZ,
BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE,
CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL,
PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,
ML, MR, NE, SN, TD, TG).

Publiée

Avec rapport de recherche internationale.

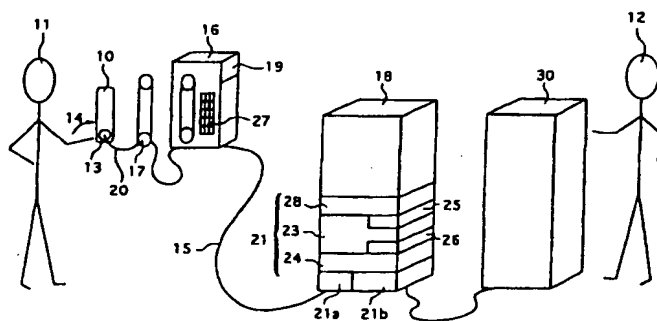
Avant l'expiration du délai prévu pour la modification des
revendications, sera republiée si de telles modifications sont
reçues.

(54) Title: METHOD AND SYSTEM FOR ENSURING THE SECURITY OF COMPUTER SERVERS OF GAMES

(54) Titre: PROCEDE ET SYSTEME POUR SECURISER LES SERVEURS INFORMATIQUES DE JEUX

(57) Abstract

The invention concerns a method and a system enabling gamesters (11) of a virtual casino to accede safely and rapidly, by means of a microphone (17) connected to a communication network (15), to the different games that the virtual casino (12) offers to its gamesters (11). The method comprises the following steps: the virtual casino provides each of its gamesters (11) with a card (10), formatted like a credit card, personalised by specific identifiers for each card and each gamester; said card (10) emits brief identifying sound signals (20), of the DTMF type, at least partly encrypted, varying with each operation, when it is actuated (14) by the gamester (11); said identifying sound signals are received by the microphone (17) and transmitted by the communication network (15) to the computer service (18) of the virtual casino; the transmitted signals and the identification data of the gamester and the card in the possession (23) of the computer service (18), are electronically processed (24) and compared (25) by the computer service (18) of the virtual casino, such that in the event of coincidence, the gamester (11) can immediately be put through to the services (30) which the virtual casino offers to the gamesters.



(57) Abrégé

L'invention concerne un procédé et un système permettant aux joueurs (11) d'un casino virtuel d'accéder de manière sûre et rapide, au moyen d'un microphone (17) relié à un réseau de communication (15), aux divers jeux que le casino virtuel (12) offre à ses joueurs (11). Le procédé comprend les étapes suivantes: le casino virtuel met à la disposition de chacun de ses joueurs (11) une carte (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque joueur; ladite carte (10) émet de brefs signaux acoustiques d'identification (20), de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée (14) par le joueur (11); lesdits signaux acoustiques d'identification sont reçus par le microphone (17) et transmis par le réseau de communication (15) au service informatique (18) du casino virtuel; les signaux transmis et les données d'identification du joueur et de la carte détenus (23) par le service informatique (18), sont traités (24) et comparés (25) électroniquement par le service informatique (18) du casino virtuel. De sorte qu'en cas de coïncidence, le joueur (11) peut être immédiatement mis en communication avec les services (30) que le casino virtuel offre aux joueurs.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Bésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LJ	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

Procédé et système pour sécuriser les serveurs informatiques de jeux.

Le domaine de l'invention est celui des prestations de service à distance.

Plus précisément l'invention concerne un procédé et un système permettant aux joueurs d'un casino virtuel (ou tous prestataires proposant des jeux : individuels ou pratiqués en groupe),
5 d'accéder de manière sûre et rapide, au moyen d'un microphone relié à un réseau de communication, aux divers jeux que le casino virtuel offre à ses joueurs.

Le problème posé est d'empêcher un utilisateur mal intentionné d'accéder au casino virtuel sans y être autorisé, sans acquitter les droits correspondants ou en prétendant qu'il n'a pas participé aux jeux d'argent qui lui sont débités par le casino virtuel.

10 Pour résoudre ce problème il a été proposé d'utiliser des clés d'accès générées par des cartes à mémoire et de modifier les combinés téléphoniques pour qu'ils puissent lire les cartes à mémoire. Ces solutions, outre leur coût, sont peu pratiques et longues à mettre en oeuvre. En fait, le problème posé ne peut être effectivement résolu que si on sait résoudre simultanément un
15 oeuvre et économique. En effet, dès lors que l'on s'adresse à un large public, la facilité d'utilisation et les gains de temps deviennent des problèmes majeurs qui ne peuvent pas être écartés.

Il a été proposé (document FR 2 702 181 au nom de Lucas GORETA, document WO 96 04741 au nom de Andrew MARK) d'utiliser une carte émettant des signaux acoustiques, cryptés, de
20 type DTMF. Ainsi, le porteur d'une telle carte, en accouplant celle-ci au microphone du combiné téléphonique transfère automatiquement ses identifiants aux services informatiques du casino virtuel. Comme ces identifiants sont chiffrés, on peut penser qu'un tiers ne sera pas en mesure d'en comprendre le contenu. Toutefois, l'enregistrement des signaux émis par la carte
25 reste possible et un fraudeur muni d'un tel enregistrement peut se substituer au bénéficiaire de la carte.

Les solutions de L. GORETA et A. MARK ne permettent donc pas d'empêcher un utilisateur mal intentionné d'accéder, sans y être autorisé, aux services informatiques du casino virtuel.

Les objectifs visés par la présente invention sont atteints et les problèmes que posent les techniques selon l'art antérieur sont résolus, selon l'invention, à l'aide d'un procédé
30 comprenant les étapes suivantes :

- le casino virtuel met à la disposition de chacun de ses joueurs une carte, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque joueur,
 - la dite carte émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée par le joueur,
- 5 - les dits signaux acoustiques d'identification sont reçus par le microphone et transmis par le réseau de communication au service informatique du casino virtuel,
- les signaux transmis et les données d'identification du joueur et de la carte détenues par le service informatique sont traités et comparés électroniquement par le service informatique du casino virtuel.
- 10 Ainsi, grâce à ce procédé, le casino virtuel peut vérifier que l'appelant dispose bien d'une carte authentique et non d'un leurre informatique. Il a pu également identifier le titulaire de la carte comme étant une personne habilitée à utiliser les services qu'il offre. De sorte qu'en cas de coïncidence, le joueur est immédiatement mis en communication avec le serveur vocal ou l'opératrice du casino virtuel. Par ailleurs, les fraudeurs n'ont plus la possibilité de dérober les
- 15 données d'identification puisque celles-ci sont transmises automatiquement sous une forme cryptée. En outre, l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par le casino virtuel. En effet, les signaux acoustiques d'identification varient à chaque opération. C'est-à-dire chaque fois que la carte est actionnée.
- 20 De préférence la dite carte :
- décompte en outre le nombre de fois $C(p,n)$ où elle est actionnée,
 - émet des signaux acoustiques représentatifs du nombre de fois $C(p,n)$ où elle a été actionnée,
 - crypte les signaux acoustiques en fonction du nombre de fois $C(p,n)$ où elle a été actionnée.
- De préférence également, les dits moyens informatiques pour traiter et comparer
- 25 électroniquement les signaux transmis et les données d'identification du joueur et de la carte détenues par le service informatique du casino virtuel,
- mémorisent le nombre de fois $C(p,m)$ où la carte a été actionnée lors de la dernière opération validée,
 - comparent le nombre de fois $C(p,n)$ où la carte a été actionnée, lors de l'opération en cours,
- 30 avec le nombre de fois mémorisé $N1$,

- rejettent l'opération en cours si $C(p,n)$ est inférieur ou égal à $C(p,m)$ et poursuivent la vérification de l'opération en cours si $C(p,n)$ est supérieur à $C(p,m)$,

- 5 - recalculent les signaux électroniques $S'(p,n)$ en fonction des données d'identification et du nombre de fois $C(p,n)$ où la carte a été actionnée, lors de l'opération en cours, puis les comparent aux signaux électroniques $S(p,n)$ transmis. De sorte qu'en cas de coïncidence, le joueur peut accéder aux jeux offerts par le casino virtuel.

Afin d'augmenter la sécurité, dans une variante de réalisation, le procédé comprend en outre l'étape suivante : le joueur émet, au moyen d'un clavier associé au combiné téléphonique et/ou à la carte, un code confidentiel. Après transmission au service informatique du casino virtuel, via
10 le réseau de communication, ce code confidentiel est traité et comparé au code confidentiel personnel du joueur détenu par le service informatique du casino virtuel.

Ainsi, le casino virtuel peut vérifier que l'appelant est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

- 15 Dans une autre variante de réalisation, afin également de renforcer la sécurité du procédé et d'éviter que le joueur ne puisse pas contester l'ordre qu'il a passé au casino virtuel, le procédé comprend en outre l'étape suivante :

- les ordres donnés par le joueur au casino virtuel sont validés par le joueur en actionnant la carte pour qu'elle émette un signal acoustique crypté de validation,
- 20 - le dit signal de validation est enregistré par le service informatique du casino virtuel.

Avantageusement, le procédé selon l'invention pourra comporter l'étape complémentaire suivante :

- un accusé de réception du signal de validation est adressé au joueur.

Grâce à ce procédé, le joueur a validé, par une signature électronique, l'ordre qu'il a donné au
25 casino virtuel.

L'invention concerne également un système permettant aux joueurs d'un casino virtuel, d'accéder de manière sûre et rapide, aux divers jeux que le casino virtuel offre à ses joueurs. Ce système a pour caractéristique de comprendre les moyens de mise en oeuvre du procédé ci-dessus défini et de ses variantes de réalisation.

- 30 Plus particulièrement:

- Le système selon l'invention comprend une carte, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque joueur, mise à la disposition de ceux-ci. La carte comporte des moyens d'émission de brefs signaux acoustiques d'identification. Ces moyens d'émission sont actionnés par le joueur au moyen d'un élément accessible de l'extérieur de la carte. La carte comporte en outre des moyens de cryptage permettant de crypter au moins en partie et de varier les signaux acoustiques chaque fois que la carte est actionnée.
- Le système selon l'invention comprend des moyens de réception et de transformation des signaux acoustiques, notamment un microphone d'un combiné téléphonique, en des signaux électroniques transmissibles à distance au moyen d'un réseau de communication,
- Le système selon l'invention comprend des moyens informatiques, dépendants du service informatique du casino virtuel, connectés au réseau de communication et situés à distance des moyens de réception des signaux acoustiques, les dits moyens informatiques comprenant :
- * une base de données contenant les références des cartes et des joueurs et leurs données d'identification,
 - * des moyens de traitement et des moyens de comparaison des signaux électroniques et des données d'identification contenues dans la base de données.
- Ainsi, grâce à ce système, le casino virtuel peut vérifier que l'appelant dispose bien d'une carte authentique et non d'un leurre informatique. Il a pu également identifier le titulaire de la carte comme étant une personne habilitée à utiliser les services qu'il offre. De sorte qu'en cas de coïncidence, le joueur est immédiatement mis en communication avec le serveur vocal ou l'opératrice du casino virtuel. Par ailleurs, les fraudeurs n'ont plus la possibilité de dérober les données d'identification puisque celles-ci sont transmises automatiquement sous une forme cryptée. En outre, l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par les services informatiques du casino virtuel. En effet, les signaux acoustiques d'identification varient à chaque opération. C'est-à-dire chaque fois que la carte est actionnée.
- De préférence la dite carte comporte en outre :
- un compteur incrémental interconnecté aux moyens d'émission et aux moyens de cryptage s'incrémentant d'au moins une unité chaque fois que la carte est actionnée.
- De sorte que l'état du compteur incrémental est émis à destination des moyens informatiques et

que les signaux acoustiques sont cryptés en fonction de l'état du compteur incrémental.

De préférence également les dits moyens informatiques comportent en outre :

- des moyens de mémorisation de l'état $C(p,m)$ du compteur incrémental lors de la dernière opération validée,

- 5 - des moyens de comparaison de l'état $C(p,n)$ du compteur incrémental émis lors de l'opération en cours avec l'état $C(p,m)$ du compteur incrémental mémorisé.

De sorte que la vérification de l'opération en cours est rejetée si $C(p,n)$ est inférieur ou égal à $C(p,m)$ et est poursuivie si $C(p,n)$ est strictement supérieur à $C(p,m)$.

- De préférence également les dits moyens de traitement et les dits moyens de comparaison des
10 signaux électroniques et des données d'identification contenues dans la base de données comportent des moyens permettant de recalculer les signaux électroniques en fonction de l'état $C(p,n)$ du compteur incrémental et des données d'identification puis de les comparer aux signaux électroniques transmis. De sorte qu'en cas de coïncidence, le joueur peut accéder immédiatement aux divers jeux offerts par le casino virtuel.

- 15 Afin d'augmenter la sécurité du système, dans une variante de réalisation, le système comprend en outre des seconds moyens de comparaison d'un code confidentiel personnel au joueur, contenu dans la base de données, à un code confidentiel émis par le joueur. Ce code est émis au moyen d'un clavier associé au combiné téléphonique et/ou à la carte et transmis aux moyens informatiques du casino virtuel, par le réseau de communication.

- 20 Ainsi, le casino virtuel peut vérifier que l'appelant est bien une personne habilitée à participer aux jeux. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

- Dans une autre variante de réalisation, afin également de renforcer la sécurité du système et d'éviter que le joueur ne puisse contester l'ordre qu'il a donné au casino virtuel, le système
25 selon l'invention est tel que :

- la dite carte émet en outre, lorsqu'elle est actionnée par le joueur du casino virtuel, un signal acoustique crypté de validation des ordres donnés par le joueur,
- les dits moyens informatiques comprennent en outre des moyens de détection et d'enregistrement du signal de validation.

- 30 Grâce à ce système, le joueur a validé, par une signature électronique, l'ordre qu'il a donné au

casino virtuel.

Avantageusement dans ce cas les moyens informatiques comprenant en outre des moyens d'édition d'un accusé de réception des ordres donnés, destiné à être adressé au joueur.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description de
5 variantes de réalisation de l'invention, données à titre d'exemple indicatif et non limitatif, et de :

- la figure 1 présentant une vue schématique en perspective du système et du procédé selon l'invention,

- la figure 2 présentant la carte sous la forme de bloc diagramme,

- la figure 3 présentant l'algorithme de vérification de l'authenticité du signal transmis.

10 Le système et le procédé selon l'invention permettent au joueur 11 d'appeler, de manière sûre et rapide, notamment au moyen d'un combiné téléphonique 16 comportant un microphone 17, les services (les divers jeux) 30 que le casino virtuel 12 met à la disposition de ses joueurs 11. Le combiné téléphonique 16, situé à distance des services informatiques 18 du casino virtuel, est connecté aux services informatiques 18 via un réseau de communication 15.

15 Le système comprend une carte 10, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et pour chaque joueur 11. Cette carte est mise à la disposition des joueurs 11 par le casino virtuel. La carte 10 comporte des moyens d'émission, notamment un haut parleur 13 émettant de brefs signaux acoustiques d'identification 20, de type DTMF. Ces signaux sont émis lorsque les moyens d'émission 13 et les organes qui les contrôlent sont
20 actionnés par le joueur au moyen d'un bouton 14 accessible de l'extérieur de la carte (non visible sur la figure 1 car situé sur l'autre côté de la carte). Ces moyens d'émission 13 sont excités par un générateur de signaux DTMF 99, contrôlé par un microprocesseur 104 alimenté par une pile 106 et piloté par un résonateur 107. Le microprocesseur 104 contenu dans la carte comporte des moyens de cryptage 103 permettant de crypter, au moins en partie, les signaux
25 acoustiques 20, comportant un algorithme de cryptage 108 et des identifiants 109 spécifiques pour chaque carte 10 et pour chaque joueur 11, notamment la clé secrète 250 utilisée par l'algorithme de cryptage 108.

Les signaux acoustiques 20 sont reçus par le microphone 17 du combiné téléphonique, contre lequel le joueur accole la carte 10. Le système comprend également des moyens de transmission
30 19 des signaux acoustiques 20, situés dans le combiné téléphonique 16. Ces moyens de

transmission 19 transmettent à distance les signaux acoustiques, après traitement et conversion en signaux électroniques, via le réseau de communication 15.

Le système comprend également des moyens informatiques 21, dépendants des services informatiques 18 du casino virtuel. Ces moyens informatiques sont connectés au réseau de communication 15 et situés à distance des combinés téléphoniques 16. Ces moyens informatiques 21 comprennent eux-mêmes :

- une base de données 23 contenant les références des cartes et des joueurs et leurs données d'identification,

- des moyens de traitement 24 et des moyens de comparaison 25 des signaux électroniques et des données d'identification contenues dans la base de données.

De sorte qu'en cas de coïncidence, les services 30 du casino virtuel sont immédiatement accessibles au joueur 11.

De préférence, le microprocesseur 104 et les moyens de cryptage 103 sont conçus de telle sorte que le signal acoustique 20 varie à chaque opération. En effet, crypter un code d'identification c'est le transformer en une suite d'informations, incompréhensibles pour tout un chacun, et que, seul le titulaire de la clef de cryptage, pourra décrypter. Mais cela n'empêche absolument pas la copie du code d'identification crypté, soit au cours de sa transmission acoustique (magnétophone), soit par piratage de la ligne téléphonique. Cette copie utilisée indûment par un fraudeur, sera traitée par le système récepteur comme ayant toutes les caractéristiques de l'original, puis interprétée afin de vérifier les identifiants de la carte.

Le problème posé est donc le suivant : comment rendre impossible toute tentative de reproduction ? Il sera ci-après décrit différentes variantes de réalisation du moyen général qui permet de faire la distinction entre l'original et la copie, lors de l'analyse du signal crypté reçu par les moyens informatiques 21, en insérant un élément distinctif dans le signal 20 du type DTMF émis par la carte 10.

L'une des variantes consiste à utiliser une fonction dite d'horodatage (par exemple, ainsi qu'elle a été décrite dans le brevet US n° 4 998 279). Cette fonction d'horodatage exploite le paramètre "temps" qui évolue en permanence. La "copie" se trouve ainsi en retard, quand elle est émise. Une telle solution nécessite une synchronisation entre les moyens d'émission 13 et les moyens informatiques 21. Pour cela tous les deux doivent disposer d'une "base de temps" et d'un

"étalon de fréquence". Ces deux bases de temps ont leur précision propre et leur dérive propre. Il en résulte qu'elles se désynchronisent lentement, mais progressivement. Pour remédier à cette difficulté technique, une certaine dérive est tolérée entre les bases de temps des moyens d'émission 13 et des moyens informatiques 21. Plus cette dérive est importante, plus l'incertitude augmente sur la "validité" de l'information reçue et plus augmente le risque de fraude. Ainsi si une dérive de une minute est tolérée, toute copie illicite de l'émission du signal crypté, et réutilisée frauduleusement dans les 30 secondes qui suivent, sera perçue comme valide par le système d'analyse des moyens informatiques 21.

Une autre variante consiste à utiliser des listes incrémentales (par exemple, ainsi qu'elle a été décrite dans le brevet US n° 4 928 098). Le dispositif d'émission et celui de réception possèdent la liste ordonnée des cryptages successifs du code d'identification ou bien disposent des algorithmes permettant de les établir au fur et à mesure. A un instant donné les moyens informatiques 21 sont en attente du résultat crypté $C(n)$. S'ils reçoivent effectivement le message $C(n)$, il valide l'opération. Mais les moyens informatiques 21 peuvent recevoir un message différent, en effet l'utilisateur de la carte peut avoir actionnée plusieurs fois les moyens d'émission 13 de celle-ci, par jeu, par maladresse, de sorte que la carte est dans la situation d'émettre le résultat crypté $C(n+p)$ lors de sa prochaine utilisation avec les moyens informatiques 21. Si les moyens informatiques 21 reçoivent un message différent, ils cherchent en avant, dans la liste des résultats cryptés successifs, s'il existe un message $C(n+p)$ identique à celui reçu. Pour lever l'ambiguïté "est-ce un message authentique émis par l'émetteur ?" ou "est-ce un message frauduleux ?", la solution consiste à demander ou à attendre l'émission suivante. Si celui-ci est alors identique à $C(n+p+1)$, le système valide alors le message et se place dans l'attente de la prochaine émission, dans l'état $C(n+p+2)$. Si celui-ci est différent, le message n'est pas validé et le système d'analyse reste en attente du message $C(n)$. Une telle variante de réalisation n'est pas très ergonomique puisqu'elle oblige le titulaire de la carte à actionner plusieurs fois celle-ci.

Selon une variante de réalisation préférentielle, pour distinguer le signal original de sa copie, le microprocesseur 104 embarqué dans la carte 10 comporte un compteur incrémental 105. A chaque usage de la carte, le compteur incrémental 105 s'incrémente d'une ou de plusieurs unités. Bien évidemment, telle une roue à cliquet, celui-ci ne peut revenir en arrière, il ne peut

qu'avancer à chaque usage.

Dans le cas de cette variante de réalisation, l'état $C(p,n)$ 242 du compteur 105 entre dans le calcul du message crypté 244 émis par les moyens d'émission 13. La partie codée $S(p,n)$ 241 est calculée par l'algorithme 108 (dont l'équivalent 247 est mémorisé dans les moyens informatiques 21 au moyen de la clé secrète 250 spécifique à chaque carte et de l'état $C(p,n)$ 242 du compteur 105. La carte 10 émet, en plus du numéro d'identification $I(p)$ 240 de la carte et du code d'identification crypté $S(p,n)$ 241, l'état $C(p,n)$ 242 de son compteur incrémental 105 à chaque émission. Les moyens informatiques 21 mémorisent 230, dans la base de données 23, l'état $C(p,n)$ 242 du compteur incrémental 105 lors de la dernière opération validée. Ainsi, à chaque réception de message 244, les moyens de comparaison 25 des moyens informatiques 21 peuvent comparer 245 l'information reçue relative à l'état $C(p,n)$ 242 du compteur 105, à la précédente information reçue $C(p,m)$ 246 et gardée en mémoire 230, 23.

a) - Si l'état $C(p,n)$ 242 du compteur 105 (fig. 2) exprimé dans le message 244 est strictement supérieur ($n > m$) à celui $C(p,m)$ 246 précédemment reçu, alors le message 244 est accepté et l'analyse se poursuit.

b)- Si l'état $C(p,n)$ 242 du compteur 105 exprimé dans le message 244 est inférieur ou égal ($n \leq m$) à celui $C(p,m)$ 246 précédemment reçu, alors le message est refusé. Le message reçu ne peut être qu'une copie antérieurement effectuée ou un leurre informatique.

Si les conditions définies au point a) ci-dessus sont réunies, les moyens informatiques 21 permettent de lire la partie fixe $I(p)$ 240 et de rechercher dans leur propre base de données 23, 230 la clé secrète correspondante de la carte. Les moyens de calcul 239 des moyens de traitement 24 peuvent alors au moyen de l'algorithme 247, de l'état du compteur $C(p,n)$ 242 et de la clé secrète $Clé(p)$ 250, procéder au calcul du code crypté attendu par les moyens informatiques 21. Le code crypté $S'(p,n)$ 248 ainsi calculé est comparé 249 à celui effectivement reçu $S(p,n)$ 241, par les moyens de comparaison 25. Ce procédé et ces moyens permettent donc de valider ou d'invalider le message 244, sans qu'il soit nécessaire à l'utilisateur de la carte d'actionner plusieurs fois celle-ci, comme cela est le cas dans la variante de réalisation ci-dessus décrite.

L'existence au sein de la carte 10 d'un compteur incrémental 105 permet, sans coût supplémentaire, de fixer, au moment de la programmation individuelle de la carte, le nombre

maximum de fois où la carte peut-être utilisée. Une fois ce maximum atteint, celle-ci n'émet plus de message cohérent et est donc refusée par les moyens informatiques 21.

La trame 244 émise contient, pour une carte donnée (p),

- une partie fixe I(p) 240 (le numéro d'identification de la carte),
- 5 - une partie variable incrémentale C(p,n) 242 (l'état du compteur),
- une partie variable S(p,n) 241 apparemment aléatoire (le résultat d'un algorithme de cryptage 108 sur la clé secrète 250 propre à cette carte (p)).

La trame émise :

- est toujours différente d'une carte à l'autre,
- 10 - est, pour une carte donnée, toujours différente à chaque émission.

Les moyens informatiques 21 permettent, pour une carte donnée (p), de :

- lire la partie fixe I(p) 240 (le numéro d'identification de la carte),
- rechercher dans leur propre base de données 23 la clé secrète 250 de cette carte et le dernier enregistrement reçu de l'état C(p,m) 246 du compteur 105 de cette carte,
- 15 - rejeter cette trame 244 si l'état du compteur C(p,n) 242 de l'opération en cours est inférieur ou égal à celui C(p,m) 246 précédemment reçu et de poursuivre la vérification de l'opération en cours si l'état C(p,n) 242 est strictement supérieur à celui C(p,m) 246 précédemment reçu,
- de "décrypter" le message 244 reçu et d'en valider le contenu, en le recalculant au moyen de l'algorithme de cryptage 247, de la clé spécifique 250 de cette carte et de l'état du compteur
- 20 C(p,n) 242, puis en comparant le résultat de ce calcul au message reçu.

Ainsi, grâce à cette combinaison de moyens il est possible d'émettre, au moyen d'une carte ayant le format d'une carte de crédit, des fréquences acoustiques de type DTMF d'identification, recevables par le microphone d'un équipement relié au réseau téléphonique, et d'avoir la certitude de l'authenticité de la carte appelante et d'écarter ainsi tous les fraudeurs utilisant tout

25 enregistrement sonore ou informatique ou tout leurre informatique.

Afin d'augmenter la sécurité du système, dans la variante de réalisation représentée sur la figure 1, les moyens informatiques 21 comprennent en outre des seconds moyens de comparaison 26. Ces moyens de comparaison permettent de comparer un code confidentiel personnel au joueur 11, contenu dans la base de données, avec le code confidentiel émis par le joueur. Ce code est

30 émis au moyen d'un clavier 27 associé au combiné téléphonique 16 et/ou à la carte 10 et

transmis aux moyens informatiques 21 du casino virtuel, par le réseau de communication. 15. Ainsi, le casino virtuel a l'assurance que l'appelant 11 est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

- 5 Dans une autre variante de réalisation, afin également de renforcer la sécurité du système et d'éviter que le joueur ne puisse contester l'ordre qu'il a donné au casino virtuel, le système selon l'invention est tel que :

- la carte 10 émet, lorsqu'elle est actionnée 14 par le joueur, un signal acoustique crypté de validation des ordres donnés par le joueur 11,

- 10 - les dits moyens informatiques 21 comprennent des moyens de détection 21a et d'enregistrement 21b du signal de validation.

Grâce à ce système, le joueur a validé, par une signature électronique, l'ordre qu'il a donné au casino virtuel.

- Avantageusement dans ce cas les moyens informatiques 21 comprennent en outre des moyens
15 d'édition 28 d'un accusé de réception 29 des ordres donnés. Cet accusé de réception est adressé au joueur 11.

REVENDICATIONS

1. Procédé permettant aux joueurs (11) d'un casino virtuel, d'accéder de manière sûre et rapide, au moyen d'un microphone (17) relié à un réseau de communication (15), aux divers jeux que le dit casino virtuel (12) offre à ses joueurs (11),

5 le dit procédé comprenant les étapes suivantes :

- le casino virtuel met à la disposition de chacun de ses joueurs (11) une carte (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque joueur,

- la dite carte (10) émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée par le joueur (11),

- les dits signaux acoustiques d'identification sont reçus par le microphone (17) et transmis par le réseau de communication (15) au service informatique (18) du casino virtuel,

- les signaux transmis et les données d'identification du joueur et de la carte détenues par le service informatique (18), sont traités (24) et comparés (25) électroniquement par le service informatique (18) du casino virtuel, de sorte qu'en cas de coïncidence les jeux du casino virtuel sont immédiatement accessibles au joueur.

2. Procédé selon la revendication 1,

20 - la dite carte (10) :

- * décompte (105) en outre le nombre de fois C(p,n) (242) où elle est actionnée par l'élément (14),

- * émet des signaux acoustiques (20) représentatifs du nombre de fois C(p,n) (242) où elle a été actionnée,

25 * crypte (103) les signaux acoustiques en fonction du nombre de fois C(p,n) (242) où elle a été actionnée,

- les dits moyens informatiques (21), pour traiter (24) et comparer (25) électroniquement les signaux transmis et les données d'identification du joueur et de la carte détenues (23) par le service informatique (18) du casino virtuel (12).

30 * mémorisent (230) le nombre de fois C(p,m) (246) où la carte a été actionnée

lors de dernière opération validée,

* comparent (245) le nombre de fois $C(p,n)$ (242) où la carte a été actionnée, lors de l'opération en cours, avec le nombre de fois mémorisé $C(p,m)$ (246),

* rejettent l'opération en cours si $C(p,n)$ (242) est inférieur ou égal à $C(p,m)$ (246) et poursuivent la vérification de l'opération en cours si $C(p,n)$ (242) est supérieur à $C(p,m)$ (246),

* recalculent (239) les signaux électroniques $S'(p,n)$ (248) en fonction des données d'identification et du nombre de fois $C(p,n)$ (242) où la carte a été actionnée, lors de l'opération en cours, puis les comparent (249) aux signaux électroniques transmis $S(p,n)$ (241), de sorte qu'en cas de coïncidence les jeux du casino virtuel sont immédiatement accessibles aux joueurs.

3. Procédé selon les revendications 1 ou 2, comprenant en outre l'étape suivante :

- le joueur émet, au moyen d'un clavier (27) associé au microphone et/ou à la carte, un code confidentiel, après transmission au service informatique (18) du casino virtuel, par le réseau de communication, ce code confidentiel est traité et comparé (26) au code confidentiel personnel du joueur détenu par le service informatique du casino virtuel.

4. Procédé selon les revendications 1, 2 ou 3, comprenant en outre l'étape suivante :

- les ordres donnés par le joueur au casino virtuel sont validés par le joueur en actionnant (14) la carte pour qu'elle émette un signal acoustique crypté de validation,
- le dit signal de validation est enregistré (21b) par le service informatique du casino virtuel.

5. Procédé selon la revendication 4, comprenant en outre l'étape suivante :

- un accusé de réception (29) du signal de validation est adressé au joueur.

6. Système permettant aux joueurs (11) d'un casino virtuel, d'accéder de manière sûre et rapide, aux divers jeux que le dit casino virtuel offre à ses joueurs, le dit système comprenant :

- une carte (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et chaque joueur, mise à la disposition de ceux-ci ; la dite carte comportant :

* des moyens (13) d'émission de brefs signaux acoustiques d'identification, de type DTMF, actionnés par le joueur du casino virtuel au moyen d'un élément accessible de

l'extérieur de la carte (10),

* des moyens de cryptage permettant de crypter au moins en partie et de varier les signaux acoustiques chaque fois que la carte est actionnée,

5 - des moyens de réception et de transformation des signaux acoustiques, notamment un microphone (17) d'un combiné téléphonique (16), en des signaux électroniques transmissibles à distance au moyen d'un réseau de communication (15),

- des moyens informatiques (21), dépendants du service informatique du casino virtuel, connectés au réseau de communication et situés à distance des moyens de réception des signaux acoustiques, les dits moyens informatiques comprenant :

10 * une base de données (23) contenant les références des cartes et des joueurs et leurs données d'identification,

* des moyens de traitement (24) et des moyens de comparaison (25) des signaux électroniques et des données d'identification contenues dans la base de données, de sorte qu'en cas de coïncidence, les jeux du casino virtuel sont immédiatement accessibles aux
15 joueurs.

7. Système selon la revendication 6,

- la dite carte (10) comportant en outre :

* un compteur incrémental (105) interconnecté aux moyens d'émission (13) et aux moyens de cryptage (103), s'incrémentant d'au moins une unité chaque fois que la carte
20 (10) est actionnée par l'élément (14), de sorte que l'état du compteur incrémental (105) est émis à destination des moyens informatiques (21) et que les signaux acoustiques sont cryptés en fonction de l'état du compteur incrémental,

- les dits moyens informatiques (21) comportant en outre :

25 * des moyens de mémorisation (23, 230) de l'état $C(p,m)$ (246) du compteur incrémental (105) lors de la dernière opération validée,

* des moyens de comparaison (245) de l'état $C(p,n)$ (242) du compteur incrémental (105) émis lors de l'opération en cours avec l'état $C(p,m)$ (246) du compteur incrémental mémorisé,

30 de sorte que la vérification de l'opération en cours est rejetée si $C(p,n)$ (242) est inférieur ou

égal à $C(p,m)$ (246) et est poursuivie si $C(p,n)$ (242) est strictement supérieur à $C(p,m)$ (246),

- les dits moyens de traitement (24) et les dits moyens de comparaison (25) des signaux électroniques et des données d'identification contenues dans la base de données comportant des moyens permettant de recalculer (239) les signaux électroniques en fonction de l'état $C(p,n)$

5 (242) du compteur incrémental (105) et des données d'identification puis de les comparer (249) aux signaux électroniques transmis,

de sorte qu'en cas de coïncidence, les jeux du casino virtuel sont immédiatement accessibles aux joueurs.

8. Système selon la revendication 7, les dits moyens informatiques comprenant en outre:

10 - des seconds moyens de comparaison (26) d'un code confidentiel personnel au joueur contenu dans la base de données, à un code confidentiel émis par le joueur au moyen d'un clavier (27) associé au combiné téléphonique et/ou à la carte et transmis aux moyens informatiques (21) du casino virtuel, par le réseau de communication (15).

9. Système selon les revendications 7 ou 8,

15 - la dite carte (10) émettant en outre, lorsqu'elle est actionnée par le joueur du casino virtuel, un signal acoustique crypté de validation des ordres donnés par le joueur,

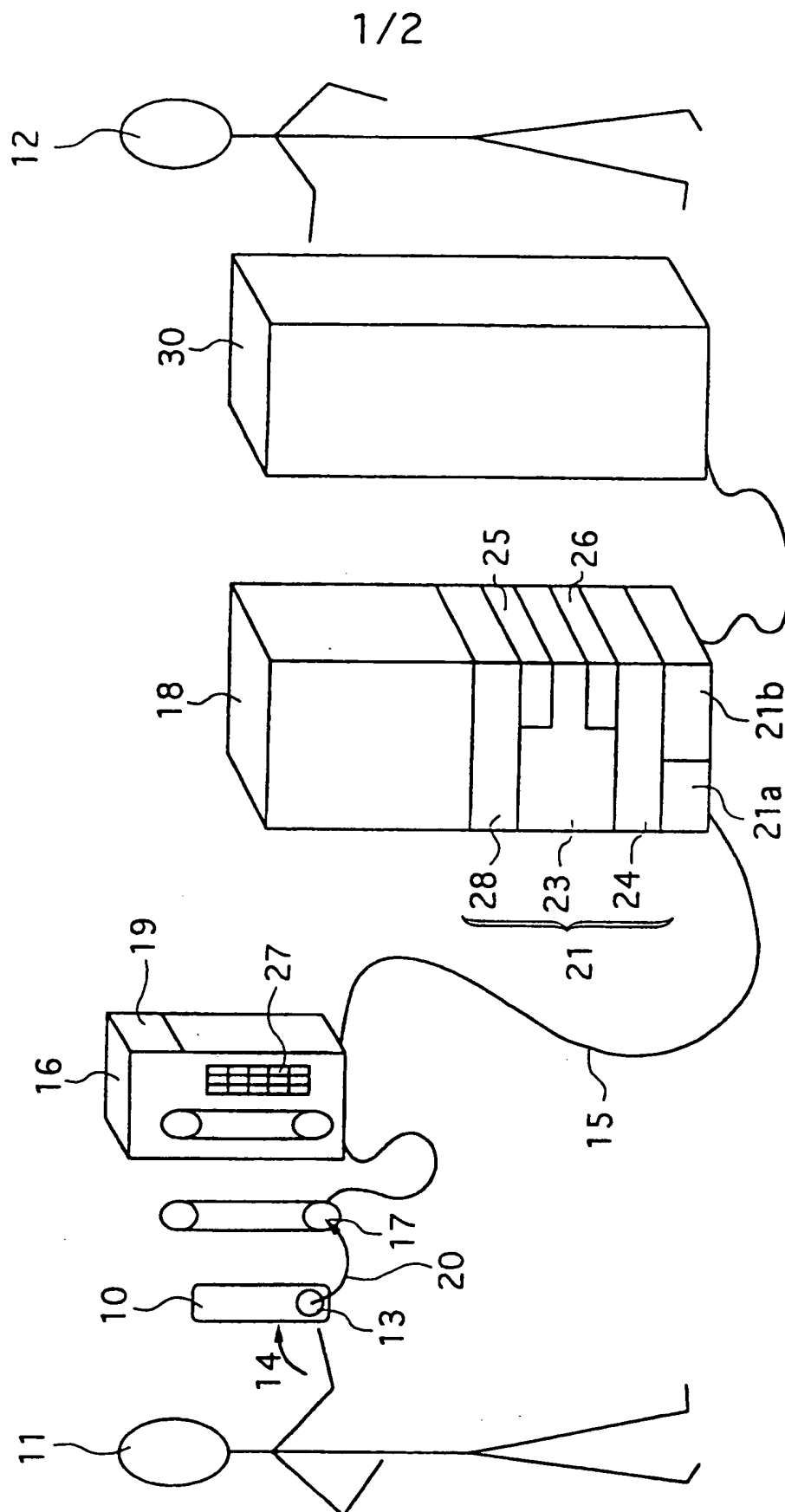
- les dits moyens informatiques comprenant en outre :

* des moyens de détection (21a) et des moyens d'enregistrement (21b) du signal de validation.

20 10. Système selon la revendication 9,

- les dits moyens informatiques comprenant en outre :

* des moyens d'édition (28) d'un accusé de réception des ordres donnés, destiné à être adressé au joueur.

Fig. 1

2/2

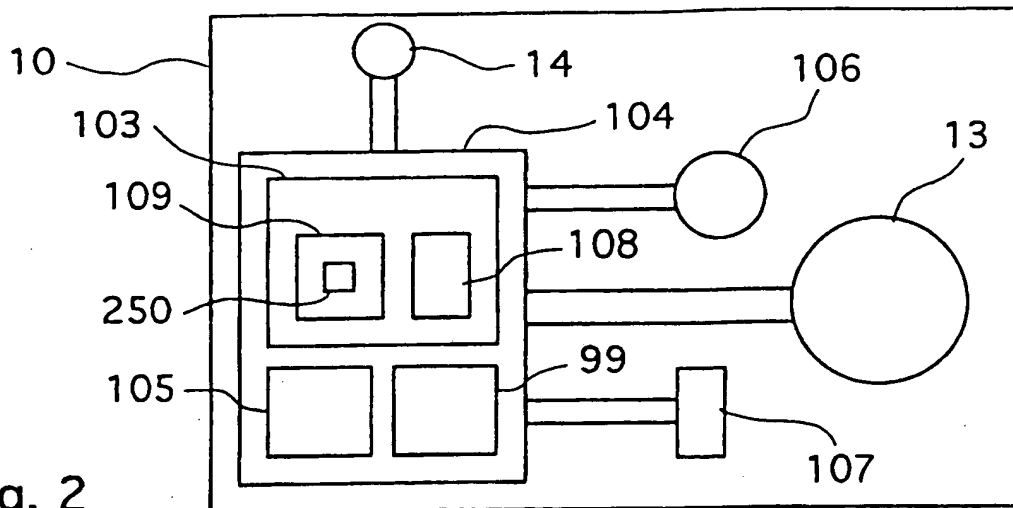


Fig. 2

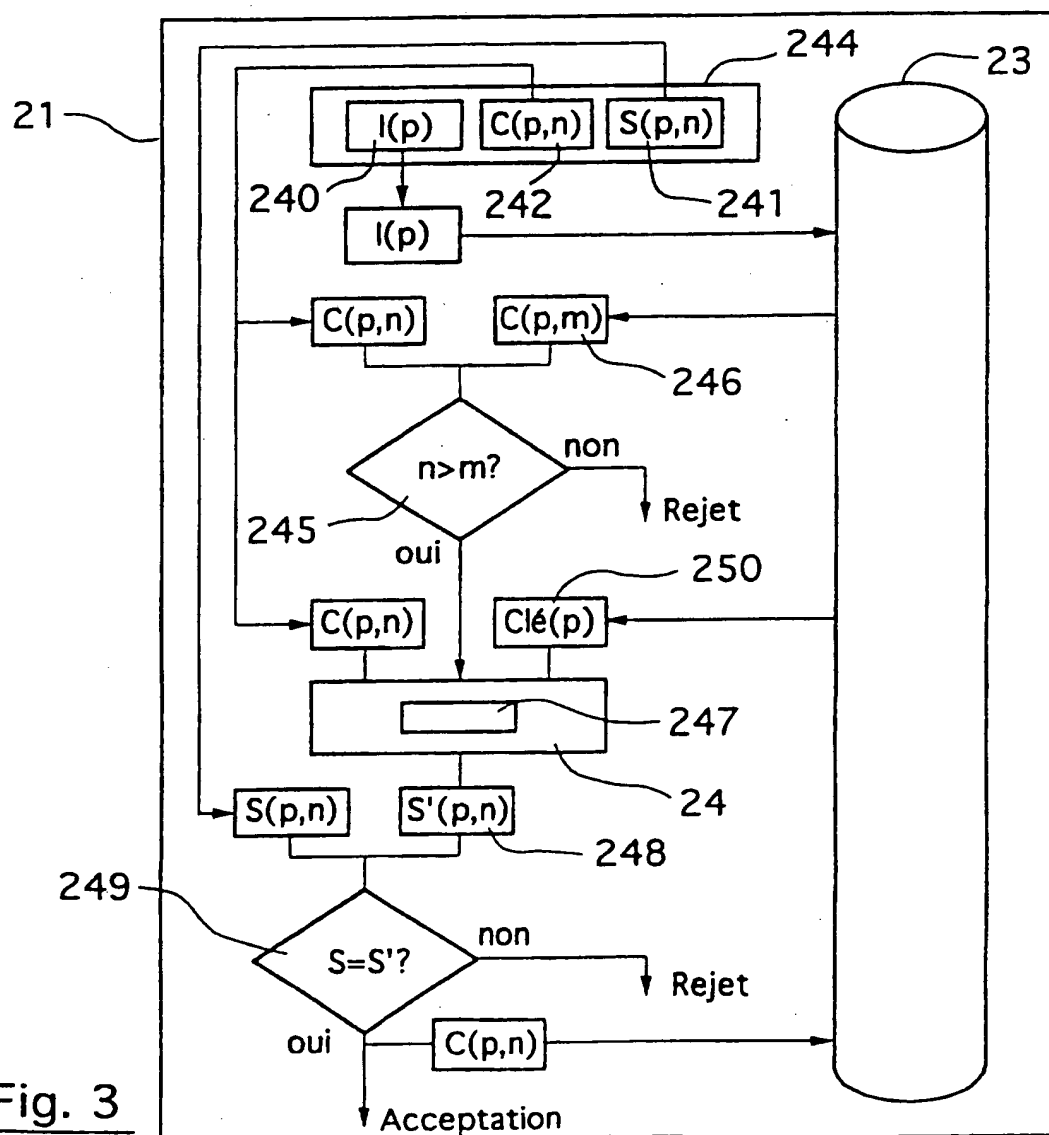


Fig. 3

INTERNATIONAL SEARCH REPORT

national Application No

PCT/FR 97/01687

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32 G07F7/10

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G07F H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	FR 2 701 181 A (GORETA) 5 August 1994 cited in the application see page 1, line 9 - line 19 see page 1, line 26 - line 43 see page 2, line 27 - line 28 see page 6, line 1 - line 7 ---	1,2,6,7
Y	EP 0 459 781 A (NANOTEQ) 4 December 1991 see column 3, line 56 - column 4, line 28 see column 5, line 20 - line 26 see column 7, line 42 - line 52 see column 9, line 48 - line 50 see column 11, line 35 - line 45 ---	1,2,6,7
Y A	GB 2 274 523 A (C. K. PATNI) 27 July 1994 see page 1, line 12 - line 25 see page 2, paragraph 4 ---	1,6 5,10
	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "Δ" document member of the same patent family

Date of the actual completion of the international search

9 February 1998

Date of mailing of the international search report

16/02/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

Application No

PCT/FR 97/01687

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 423 035 A (GEMPLUS) 17 April 1991 see column 1, line 45 - column 3, line 28 see column 5, line 25 - line 42 ----	2,7
A	DE 43 25 459 A (EISELE) 9 February 1995 see column 2, line 25 - column 3, line 22 see column 4, line 45 - line 55 -----	3,4,8,9

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 97/01687

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2701181 A	05-08-94	NONE	
EP 459781 A	04-12-91	AT 136975 T DE 69118748 D DE 69118748 T ES 2085425 T US 5517187 A	15-05-96 23-05-96 28-11-96 01-06-96 14-05-96
GB 2274523 A	27-07-94	NONE	
EP 423035 A	17-04-91	FR 2653248 A CA 2027344 A,C DE 69014817 D DE 69014817 T ES 2066169 T JP 1884135 C JP 3241463 A JP 6009051 B US 5191193 A	19-04-91 14-04-91 19-01-95 22-06-95 01-03-95 10-11-94 28-10-91 02-02-94 02-03-93
DE 4325459 A	09-02-95	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Internationale No
PCT/FR 97/01687

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04L9/32 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 H04L G07F H04M

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	FR 2 701 181 A (GORETA) 5 août 1994 cité dans la demande voir page 1, ligne 9 - ligne 19 voir page 1, ligne 26 - ligne 43 voir page 2, ligne 27 - ligne 28 voir page 6, ligne 1 - ligne 7 ---	1,2,6,7
Y	EP 0 459 781 A (NANOTEQ) 4 décembre 1991 voir colonne 3, ligne 56 - colonne 4, ligne 28 voir colonne 5, ligne 20 - ligne 26 voir colonne 7, ligne 42 - ligne 52 voir colonne 9, ligne 48 - ligne 50 voir colonne 11, ligne 35 - ligne 45 --- -/--	1,2,6,7

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (elle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

9 février 1998

Date d'expédition du présent rapport de recherche internationale

16/02/1998

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

bande internationale No

PCT/FR 97/01687

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	GB 2 274 523 A (C. K. PATNI) 27 juillet 1994	1,6
A	voir page 1, ligne 12 - ligne 25 voir page 2, alinéa 4	5,10
A	EP 0 423 035 A (GEMPLUS) 17 avril 1991 voir colonne 1, ligne 45 - colonne 3, ligne 28 voir colonne 5, ligne 25 - ligne 42	2,7
A	DE 43 25 459 A (EISELE) 9 février 1995 voir colonne 2, ligne 25 - colonne 3, ligne 22 voir colonne 4, ligne 45 - ligne 55	3,4,8,9

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Recherche Internationale No
PCT/FR 97/01687

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2701181 A	05-08-94	AUCUN	
EP 459781 A	04-12-91	AT 136975 T DE 69118748 D DE 69118748 T ES 2085425 T US 5517187 A	15-05-96 23-05-96 28-11-96 01-06-96 14-05-96
GB 2274523 A	27-07-94	AUCUN	
EP 423035 A	17-04-91	FR 2653248 A CA 2027344 A,C DE 69014817 D DE 69014817 T ES 2066169 T JP 1884135 C JP 3241463 A JP 6009051 B US 5191193 A	19-04-91 14-04-91 19-01-95 22-06-95 01-03-95 10-11-94 28-10-91 02-02-94 02-03-93
DE 4325459 A	09-02-95	AUCUN	

